

PORTARIA 02/2014
DIRETORIA EXECUTIVA
FUNDAÇÃO JOÃO PAULO II

Dispõe sobre a criação e instituição do Regulamento de Segurança da Informação na Fundação João Paulo II e sua aplicabilidade.

O Diretor Executivo da **FUNDAÇÃO JOÃO PAULO II**, com a proteção de Deus e rogando a proteção da Virgem Maria, no uso das atribuições que lhe conferem os incisos I, IV, VII, do artigo 55 do Estatuto Social da entidade, e

Considerando a necessidade de garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das informações necessárias para a realização dos negócios da Fundação João Paulo II,

Considerando a existência do Manual de Orientação de Conduta da Fundação João Paulo II e a necessidade de um detalhamento de sua política de Segurança da Informação, utilização de meios eletrônicos, internet e confidencialidade, **resolve instituir o:**

Regulamento de Segurança da Informação
Fundação João Paulo II

BASEADA NA NORMA ABNT 21:204.01-010

Este regulamento de segurança da informação, na Fundação João Paulo II, aplica-se a todos os funcionários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da Fundação João Paulo II, ou acesso a informações pertencentes à empresa. Todo e qualquer usuário de recursos computadorizados da Fundação João Paulo II tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática. A violação desta política de segurança é qualquer ato que:

1. *Exponha a Fundação João Paulo II a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.*
2. *Envolve a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.*
3. *Envolve o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.*

ART. 1º – DOS OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das informações necessárias para a realização do negócio da Fundação João Paulo II.

ART. 2º - DA MISSÃO DO SETOR DE TECNOLOGIA DA INFORMAÇÃO: Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das informações necessárias para a realização do negócio da Fundação João Paulo II. Ser o gestor do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou

implementando ações para esta finalidade.

ART. 3º - DOS DEVERES DE TODOS NA EMPRESA: Considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a Fundação João Paulo II e deve sempre ser tratada profissionalmente.

Parágrafo Único – Caberá aos Superintendentes de cada área a missão de fiscalizar o cumprimento deste regulamento, bem como zelar pela sua aplicação, com a promoção de treinamentos e reuniões.

ART. 4º - DA CLASSIFICAÇÃO DA INFORMAÇÃO: É de responsabilidade do Gerente/Supervisor de cada área estabelecer e comunicar seus subordinados critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

1 – Pública

2 – Interna

3 – Confidencial

4 – Restrita

Parágrafo Único – Conceitos:

- a) **Informação Pública:** É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.
- b) **Informação Interna:** É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.
- c) **Informação Confidencial:** É toda informação que não pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.
- d) **Informação Restrita:** É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização. Todo Gerente/Supervisor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

ART. 5º – DOS DADOS DOS FUNCIONÁRIOS: A Fundação João Paulo II se compromete em não acumular ou manter intencionalmente dados pessoais de funcionários, além daqueles relevantes na condução do seu negócio. Todos os dados pessoais de funcionários que porventura sejam armazenados, serão considerados dados confidenciais e sob a responsabilidade da Fundação João Paulo II, não serão usados para fins diferentes daqueles para os quais foram coletados.

Parágrafo Único - Dados pessoais de funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que devidamente autorizado pelo setor jurídico e tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários da organização.

ART. 6º - DO ARMAZENAMENTO DE DADOS PARTICULARES: Os funcionários se comprometem a não armazenar dados particulares nas instalações da empresa, assim como em computadores e dispositivos eletrônicos (pendrive, hd externo, cd...) sem prévia e expressa autorização por parte da diretoria e/ou Supervisão/Gerencia.

Parágrafo Primeiro - Mesmo que seja autorizado o armazenamento destes dados, a empresa não se responsabiliza por eles, nem tampouco pelo seu conteúdo e pela segurança. Tais dados jamais poderão ser armazenados nos diretórios dos Servidores de empresa, e jamais poderão fazer parte da rotina de backup da empresa.

Parágrafo Segundo – Ressalta-se que o uso de qualquer equipamento (como notebooks, pendrives, hd externo, cartões de memória...) é somente para o trabalho.

ART. 7º - DA ADMISSÃO, DEMISSÃO E TRANSFERENCIA DE FUNCIONÁRIOS / TEMPORÁRIOS / ESTAGIÁRIOS: O setor de RH da Companhia deverá informar ao setor de TI, toda e qualquer movimentação de temporários e/ou estagiários, bem como admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou excluídos no sistema da empresa.

Parágrafo Primeiro - Todo 2º (segundo) dia útil de cada mês, o setor de RH deve encaminhar para o setor de TI uma lista com os nomes, para que sejam feitos os ajustes assim como liberações no sistema.

Parágrafo Segundo - Ressalta-se, que nas situações de transferência de colaboradores, o setor de RH deve informar ao setor de TI todos os dados referentes ao setor que o colaborador estava e do novo setor no qual ele estará atuando, para que sejam providenciadas liberações e/ou restrições de acesso.

Parágrafo Terceiro - O ato de desligamento e/ou transferência de um colaborador, o backup de dados é de responsabilidade do setor de TI.

ART. 8º - DOS PROGRAMAS ILEGAIS: A Fundação João Paulo II respeita os direitos autorais dos programas que usa e reconhece que deve pagar o justo valor por eles, não autorizando o uso de programas não licenciados nos computadores da empresa. É terminantemente proibido o uso de programas ilegais (Sem licenciamento) na Fundação João Paulo II.

Parágrafo Primeiro - Os usuários não podem, em hipótese alguma, instalar este tipo de "software" (programa) nos equipamentos da empresa, mesmo porque somente o setor de TI tem autorização para instalação de programas, previamente autorizados dentro da política de segurança da companhia. Periodicamente, o Setor de TI fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz. Caso sejam encontrados programas não autorizados, estes deverão ser removidos.

Parágrafo Segundo - Aqueles que instalarem em seus computadores de trabalho tais programas não autorizados, se responsabilizam perante a companhia por quaisquer problemas ou prejuízos causados oriundos desta ação, estando sujeitos as sanções previstas neste documento.

ART. 9º - DAS PERMISSÕES E SENHAS: Todo usuário para acessar os dados da rede da Fundação João Paulo II, deverá possuir um login e senha previamente cadastrados e liberados pelo departamento de TI.

Parágrafo Primeiro - Quem deve fornecer os dados referente aos direitos (privilégios de acesso) do usuário é o responsável direto. O departamento de TI fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada imediatamente após o primeiro login e após isso a cada 45 (quarenta e cinco) dias. Nesse primeiro momento, essa regra não se aplica as máquinas Windows que estão fora do domínio (Casas de Missão).

Parágrafo Segundo - Por segurança, a área de TI recomenda que as senhas tenham sempre um critério mínimo de segurança para que não sejam facilmente copiadas, e não possam ser repetidas.

Parágrafo Terceiro - POLÍTICAS DE SENHAS:

- a) Uma senha segura deverá conter no mínimo 6 caracteres alfanuméricos (letras e números) com diferentes caixas (letra maiúscula e minúscula);
- b) Para facilitar a memorização das senhas, utilize padrões mnemônicos. Por exemplo: eSus6C (eu SEMPRE uso seis 6 CARACTERES) e odlamp0709 (ouviram do Ipiranga as margens plácidas 7 de Setembro);
- c) As senhas terão um tempo de vida útil determinado pela equipe de segurança, devendo o mesmo ser respeitado;
- d) A senha não deve ser jamais passada a ninguém, nem mesmo da equipe de segurança. Caso desconfie que sua senha não está mais segura, sinta-se à vontade para alterá-la, mesmo antes do prazo determinado de validade;
- e) Tudo que for executado com a sua senha será de sua inteira responsabilidade, por isso tome todas as precauções possíveis para manter sua senha secreta.;
- f) Todos os usuários responsáveis pela aprovação eletrônica de documentos (exemplo: pedidos de compra, solicitações e etc) deverão comunicar ao Setor de TI/Sistemas qual será o seu substituto quando de sua ausência da Fundação João Paulo II, para que as permissões possam ser alteradas (delegação de poderes). Quando houver necessidade de acesso para usuários externos, sejam eles temporários ou não, a permissão de acesso deverá ser bloqueada tão logo este tenha terminado o seu trabalho e se houver no futuro nova necessidade de acesso, deverá então ser desbloqueada pelo pessoal de TI.

ART. 10 – DO COMPARTILHAMENTO DE DADOS: Não é permitido o compartilhamento de pastas nos computadores e desktops da Fundação João Paulo II. Todos os dados deverão ser armazenados nos Servidores da rede, e a autorização para acessá-los deverá ser fornecida pelo setor de TI, que está orientado a periodicamente verificar todos os arquivos existentes nas estações de trabalho e garantir que dados considerados confidenciais e/ou restritos não estejam armazenados na rede e sim nos servidores.

Parágrafo Único - Os compartilhamentos de impressoras devem estar sujeitos as autorizações de acesso. Não são permitidos na Fundação João Paulo II o compartilhamento de dispositivos móveis tais como pen-drivers e outros.

ART. 11 – DO ARMAZENAMENTO DE ARQUIVOS EM DESKTOPS: Não é política da Fundação João Paulo II o armazenamento de dados em desktops individuais, entretanto, existem alguns programas fiscais que não permitem o armazenamento em rede. Nestes e em outros casos, os dados devem ser salvos na opção “Meus Documentos” do computador só usuários, e o setor de TI deverá estar ciente e alertar ao usuário que ele deve fazer e orientar quanto a backup dos dados de sua máquina periodicamente. Sendo assim, todos os dados considerados importantes para o trabalho devem ser armazenados na opção “Meus Documentos” do computador do usuário, para que dessa forma tais informações sejam incluídas na rotina diária de backup da TI.

Parágrafo Único - É responsabilidade dos próprios usuários a elaboração de cópias de segurança (“backups”) de dados e outros arquivos ou documentos particulares, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da Fundação João Paulo II.

ART. 12 - DA SEGURANÇA E INTEGRIDADE DOS DADOS: O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva do Setor de TI, assim como a manutenção, alteração e atualização de equipamentos e programas.

ART. 13 - DA PROPRIEDADE INTELECTUAL: É de propriedade da Fundação João Paulo II, todos os “designs”, criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a Fundação João Paulo II.

ART. 14 - DO ACESSO À INTERNET: O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na Fundação João Paulo II. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados. O uso da Internet será monitorado pelo Setor de TI, inclusive através de “logs” (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

Parágrafo Único - A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição dos Supervisores/Gerentes, com base em recomendação do Supervisor de TI. Não é permitido instalar programas provenientes da Internet nos microcomputadores da Fundação João Paulo II, sem expressa anuência do setor de TI, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais. Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros. Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso dos seguintes sites:

- a) De estações de rádio;
- b) De conteúdo pornográfico ou relacionados a sexo;
- c) Que defendam atividades ilegais;
- d) Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- e) Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da Fundação João Paulo II;
- f) Que promovam discussão pública sobre os negócios da Fundação João Paulo II, a menos que autorizado pela Diretoria;
- g) Que possibilitem a distribuição de informações de nível “Confidencial”;
- h) Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.
- i) É proibido o uso de IM (Instant messengers) não homologados/autorizados pela equipe de segurança do departamento de TI.

ART. 15 - DO USO DO CORREIO ELETRÔNICO (E-MAIL): O correio eletrônico fornecido pela Fundação João Paulo II é um instrumento de comunicação interna e externa para a realização do negócio empresa, devendo ser utilizado somente pelos usuários que realmente necessitem dessa ferramenta, a necessidade de utilização deve ser levantada pelo gerente/supervisor e a autorização para acessá-los deverá ser fornecida pelo setor de TI.

Parágrafo Primeiro - A criação do e-mail por parte do setor de TI, deve obedecer padrões externos (baseados nas normas vigentes) que orientam a utilização de nome.sobrenome@empresa.com, por exemplo: jose.silva@cancaonova.com.

Parágrafo Segundo - Não será permitido o acesso a e-mails particulares nos computadores da Fundação João Paulo II, tampouco envio de informações particulares referente a empresa através desses e-mails particulares.

a) Quanto às mensagens, as mesmas:

- Devem ser escritas em linguagem profissional;
- Não devem comprometer a imagem da Fundação João Paulo II;
- Não podem ser contrárias à legislação vigente nem aos princípios éticos da Fundação João Paulo II;

b) O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis e inúteis;
- Sejam relativas a "correntes", de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da organização;
- Possam prejudicar a imagem de outras empresas;
- Sejam incoerentes com as políticas da Fundação João Paulo II.

Parágrafo Terceiro - Para incluir um novo usuário no correio eletrônico, a respectiva Gerência deverá através do facilitador de RH, fazer um pedido formal ao Setor de TI/Datacenter, que providenciará a inclusão do mesmo. A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado. Em caso de congestionamento no Sistema de correio eletrônico o Setor de TI fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo.

Parágrafo Quarto - Não será permitido o uso de e-mail gratuitos (liberados em alguns sites da web), nos computadores da Fundação João Paulo II. O Setor de TI poderá barrar o acesso a esses sites, visando evitar a entrada de vírus na empresa, além de bloquear o recebimento de e-mails provenientes de sites gratuitos.

ART. 16 - DA NECESSIDADE DE NOVOS SISTEMAS, APLICATIVOS E EQUIPAMENTOS: O Setor de TI é responsável pela aplicação da Norma da Fundação João Paulo II, em relação a definição de compra e substituição de "software" e "hardware". Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pelo setor (supervisor/gerente). Não é permitido a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos usuários.

Parágrafo Único - Após aprovação da necessidade de compra por parte do supervisor/gerente, o facilitador de RH com base em um documento de solicitação de compra, deve abrir um chamado (ticket) explicando ao setor de TI a sua necessidade. Por outro lado, o setor de TI deve verificar o histórico e padrões de compra, e assim retornar o ticket com a descrição de equipamentos e/ou softwares para dar continuidade a compra junto ao setor responsável.

ART. 17 - DO USO DE LAPTOPS/NOTEBOOKS (COMPUTADORES PESSOAIS) NA EMPRESA: O uso de notebooks particulares não é permitido dentro da Fundação João Paulo II, exceto perante identificação e justificativa da necessidade por parte do gerente e liberação e autorização do supervisor de TI. Após esse processo de liberação, o usuário deve procurar o setor de TI levando o seu equipamento, para que possa juntamente com seu responsável assinar um termo de responsabilidade.

ART. 18 – DOS SISTEMAS DE TELECOMUNICAÇÕES (TELEFONIA): O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da Fundação João Paulo II, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do setor de Telefonia juntamente com o setor de Informática, de acordo com as definições da Diretoria da Fundação João Paulo II. Ao final de cada mês, para controle, serão enviados relatórios informando a cada gerência quanto foi gasto por cada ramal, sendo assim é importante ressaltar que:

Parágrafo Único - O telefone é um recurso fornecido pela Fundação João Paulo II, como mais uma ferramenta de comunicação. Sendo assim, o mesmo deve ser utilizado com responsabilidade e somente para assuntos de trabalho. Caso seja necessário fazer alguma ligação particular, isto deve ser informado ao telefonista juntamente com o número de identificação do colaborador (crachá).

ART. 19 – DO USO DE IMPRESSORAS: O uso de serviços de impressão deve ser utilizado somente para fins de trabalho. Sendo vedado o uso para qualquer tipo de impressões particulares.

ART. 20 – DO USO DE ANTIVIRUS: Todo arquivo em mídia proveniente de entidade externa a Fundação João Paulo II, assim como da Internet deve ser verificado por programa antivírus. Todas as estações de trabalho devem possuir um antivírus instalado, e sua atualização será automática, agendada pelo setor de TI via rede. O usuário não pode em hipótese alguma desabilitar o programa antivírus instalado em sua estação de trabalho.

ART. 21 – DA RESPONSABILIDADE DOS GERENTES / SUPERVISORES: Os gerentes e supervisores são responsáveis pelas definições dos direitos de acesso (privilégios) de seus funcionários aos sistemas, equipamentos e informações da Companhia, cabendo a eles identificar e solucionar as necessidades dos seus funcionários, além de verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, conforme estabelecido neste regulamento.

Parágrafo Único: O Setor de TI fará auditorias periódicas do acesso dos usuários às informações, verificando:

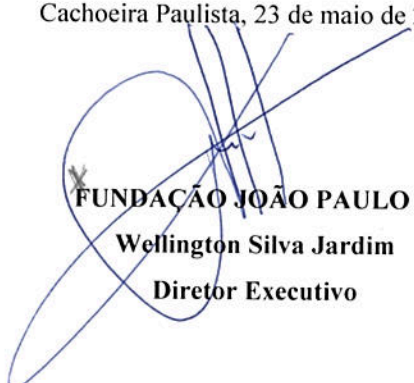
- a) Que tipo de informação o usuário pode acessar;
- b) Quem está autorizado a acessar determinada rotina e/ou informação;
- c) Quem acessou determinada rotina e informação;
- d) Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;
- e) Que informação ou rotina determinado usuário acessou;
- f) Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

ART. 22 - DA REVISÃO/ATUALIZAÇÃO: A fim de manter atualizadas todas as informações contidas nesse documento, o mesmo será revisado periodicamente a cada 5 (cinco) meses, para que sejam feitas as devidas adequações.

ART. 23 – DAS PENALIDADES: O não cumprimento deste Regulamento de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência verbal, advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

Esta Portaria e o respectivo Regulamento entram em vigor na data de sua publicação, dando-se ciência a todos os colaboradores da entidade, sem exceção e aos órgãos externos de controle e a Curadoria das Fundações.

Cachoeira Paulista, 23 de maio de 2014.


FUNDACÃO JOÃO PAULO II
Wellington Silva Jardim
Diretor Executivo